UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/555,891	11/07/2005	Alessandro Bruti	09952.0011-00000	2722

22852   7590   12/30/2008
FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER
LLP
901 NEW YORK AVENUE, NW
WASHINGTON, DC 20001-4413

EXAMINER
KANAAN, SIMON P

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
12/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>07 November 2005</u>.
2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>33-64</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>33-64</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>07 November 2005</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
       1.☒ Certified copies of the priority documents have been received.
       2.☐ Certified copies of the priority documents have been received in Application No. _____.
       3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>May 30, 2007, April 25, 2006, Nov. 7, 2005.</u>

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____ .

DETAILED ACTION

1.   The instant application having Application No. 10/555891 filed on 11/7/2005 is

presented for examination by the examiner.

Claims 1 through 32 canceled by applicant. Claims 33 through 64 are pending.

Examiner Notes

2.   Examiner cites particular columns and line numbers in the references as applied

to the claims below for the convenience of the applicant. Although the specified citations

are representative of the teachings in the art and are applied to the specific limitations

within the individual claim, other passages and figures may apply as well. It is

respectfully requested that, in preparing responses, the applicant fully consider the

references in entirety as potentially teaching all or part of the claimed invention, as well

as the context of the passage as taught by the prior art or disclosed by the examiner.

Oath/Declaration

3.   The applicant's oath/declaration has been reviewed by the examiner and is found

to conform to the requirements prescribed in **37 C.F.R. 1.63.**

Priority

4.   As required bye **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's

claim for priority based on applications filed on May 13, 2003 (IT 2003/00284).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which

papers have been placed of record in the file.

Drawings

5.   The applicant's drawings submitted are acceptable for examination purposes.

Information Disclosure Statement

6.   The information disclosure statement (IDS) submitted on October 29, 2008 has

been acknowledged. The submission is in compliance with the provisions of 37

CFR 1.97. Accordingly, the information disclosure statement is being considered by the

examiner.

Claim Rejections - 35 USC § 101

7.   35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of
matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and
requirements of this title.

8.   Claim 64 is rejected under 35 U.S.C. 101 as directed o non-statutory subject

matter of software, *per se*. The claim lacks the necessary physical articles or objects to

constitute a machine or manufacture within the meaning of 35 U.S.C. 101. It is clearly

not a series of steps or acts to be a process nor are they a combination of chemical

compounds to be a composition of matter. As such, they fail to fall within a statutory

category. It is at best, function descriptive material *per se*.

In this case, applicant has claimed a "a program product" for causing a computer

to execute instructions in the preamble to these claims; this implies that Applicant is

claiming a system of software, per se, lacking the hardware necessary to realize any of

the underlying functionality. Therefore, claim 65 is directed to non-statutory subject

matter as computer programs, per se, i.e. the descriptions or expressions of the

programs, are not physical "things." They are neither computer components nor

statutory processes, as they are not "acts" being performed. Such claimed computer

programs do not define any structural and functional interrelationships between the

computer program and other claimed elements of a computer, which permit the

computer program's functionality to be realized.

Claim Rejections - 35 USC § 112

9.   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly
> claiming the subject matter which the applicant regards as his invention.

10.   Claims 43 and 44 are rejected under 35 U.S.C. 112, second paragraph, as being

indefinite for failing to particularly point out and distinctly claim the subject matter which

applicant regards as the invention.

Claim 43 recites the limitation "step of fragmenting" in line 1 of the claim. There

is insufficient antecedent basis for this limitation in the claim.

Claim 44 recites the limitation "step of each terminal in said group authenticating

themselves" in lines 1 and 2 of the claim. There is insufficient antecedent basis for this

limitation in the claim.

Claim Rejections - 35 USC § 103

11. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

12. Claims 33 through 47 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Enhanced Protection over Wireless Lans (copyright February 2000,

NoWiresNeeded) hereinafter called EPWL in view of Kim et al. Simple and fault-

Tolerant Agreement for Dynamic Collaborative Groups (by Kim, Perrig and Tsudik

copyright 2000 ACM) hereinafter called Kim.

13. As per claim 33, EPWL discloses "A process for secure communication over a

wireless network including a group of terminals," *(EPWL, page 6, right hand column,*

lines 19 through 25, client and access points, i.e. terminals, communicate in a security

enhanced 802.11 authentication protocol, hence communicate over a wireless network)

"wherein such terminals exchange information ciphered by means of at least one key,

comprising the step of generating said at least one key independently at each said

terminal in said group ." *(EPWL, page 6, right hand column, lines 10 through 12, each*

station i.e. terminal generates an encryption key using the Diffie-Hellman key

agreement algorithm) but fails to disclose expressly "by means of a protocol of the

group key agreement type." *(Kim, page 235, right hand column, lines 30 through 34,*

group key management protocols are used)

Kim discloses "by means of a protocol of the group key agreement type." *(Kim,*

page 235, right hand column, lines 30 through 34, group key management protocols are

used)

EPWL and Kim are analogous art because they are from the same field of

endeavor of wireless communication.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to incorporate the method for secure key exchange as described by EPWL

and the group key agreement method as taught by Kim because group key prevents

network from a single point of failure and therefore less attractive for attack *(Kim, page*

235, lines 14 through 18).

As per claim 34, EPWL in view of Kim discloses: "The process of claim 33,

comprising the steps of: generating, at each said terminal in said group, respective

secret local data and maintaining said local data secret at said terminal; *(EPWL, page 6,*

right hand column, lines 10 through 12, each station i.e. terminal generates an

encryption key using the Diffie-Hellman key agreement algorithm, this encryption key is

secret data) exchanging publicly accessible information among the terminals in said

group; *(EPWL, page 6, right hand column, lines 7 through 8, each station i.e. terminal exchanges data without a need for secure a channel hence publicly accessible information is exchanged among terminals in said group)* and generating, independently at each said terminal in the group, said at least one key on the basis of said respective local data maintained secret at each said terminal and said publicly accessible information." *(EPWL, page 6, right hand column, lines 7 through 16, each station i.e. terminal generates an encryption key using the Diffie-Hellman key agreement algorithm from the information exchanged)*

As per claim 35, EPWL in view of Kim discloses: "The process of claim 34, comprising the step of incorporating to said publicly accessible information coded information representative of each terminal in said group, whereby generation of said at least one key is contributed by all the terminals in said group." *(Kim, page 238, right hand column, lines 1 through 10, each member generates its own key which is a part of the group key, since each member knows the other keys on the path each generates an intermediate key the root will create the root will create the group key)*

As per claim 36, EPWL in view of Kim discloses: "The process of claim 35, comprising the steps of: encoding each terminal in said group by means of respective labels; and generating a vector of the labels of all the terminals in said group, *(Kim, page 238, left hand column, lines 43 through 50, each member can compute and stores the identical tree which is the structure of the group, a tree is a vector)* wherein said

vector is included in said publicly accessible information exchanged among the

terminals in said group." *(Kim, page 239, left hand column, lines 1 through 5, sponsor*

broadcasts the tree)

As per claim 37, EPWL in view of Kim discloses: "The process of claim 34,

wherein publicly accessible information exchanged among terminals in said group is

representative of a tree-structure for generating said at least one key." *(Kim, page 238,*

right hand column, lines 1 through 10, each member generates its own key which is a

part of the group key, each member knows all the keys from the path of its leaf)

As per claim 38, EPWL in view of Kim discloses: "The process of claim 33,

comprising the step of generating said at least one key independently at each said

terminal in said group by means of a Diffie- Hellman group algorithm." *(EPWL, page 6,*

right hand column, lines 10 through 13, each station i.e. terminal generates an

encryption key using the Diffie-Hellman key agreement algorithm)

As per claim 39, EPWL in view of Kim discloses: "The process of claim 38,

wherein said algorithm is the TGDH algorithm." *(Kim, page 238, left hand column, line*

21, TGDH algorithm protocols used)

As per claim 40, EPWL in view of Kim discloses: "The process of claim 33,

comprising the step of each terminal in said group authenticating itself by means of

digital authentication information." *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digitally authenticated)*

As per claim 41, EPWL in view of Kim discloses: "The process of claim 40, comprising the step of each terminal in said group authenticating itself by means of a digital certificate." *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digital certificate)*

As per claim 42, EPWL in view of Kim discloses: "The process of claim 34, comprising the step of exchanging said publicly accessible information by means of information packets." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via packets since it uses TCP/IP)*

As per claim 43, EPWL in view of Kim discloses: "The process of claim 42, comprising the step of fragmenting said publicly accessible information over a plurality of information packets." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via TCP/IP, packets in TCP are fragmented into the IP layer)*

As per claim 44, EPWL in view of Kim discloses: "The process of claim 34, comprising the steps of each terminal in said group authenticating themselves by means of digital authentication information, *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digitally authenticated)* fragmenting said publicly accessible information over a plurality of information packets and associating said authentication information with all of said packets." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via TCP/IP, packets in TCP are fragmented into the IP layer)*

As per claim 45, EPWL in view of Kim discloses: "The process of claim 34, comprising the steps of each terminal in said group authenticating themselves by means of digital authentication information, *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digitally authenticated)* fragmenting said publicly accessible information over a plurality of information packets and including said digital authentication information with one of said packets, whereby the remaining part of said plurality of packets comprises a lower protocol layer conveying information resulting from said fragmentation." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via TCP/IP, packets in TCP are fragmented into the IP layer, hence*

creating a plurality of packets at a lower protocol)

As per claim 46, EPWL in view of Kim discloses: "The process of claim 33, comprising the step of configuring said each terminal in said group for generating at least one message selected from the group of: a join message generated when said terminal enters said group and conveying information that merged with other information provided by all the other terminals in said group is adapted to generate said at least one key; *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor updates the tree and computes the new group key and broadcasts it)* a key message generated during the generation of said at least one key and containing data that respective terminals other than a new terminal joining said group have to provide for generating said at least one key; *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor updates the tree and computes the new group key and broadcasts it, the sponsor can compute the new group key since it knows all the necessary blinded keys)* and a leave message generated to notify the other terminals in said group that the source terminal is leaving the group." *(Kim, page 239, section 5.3, when a member leaves new group key is computed by sponsor and broadcasted so other members can compute the knew group key and update the tree accordingly)*

As per claim 47, EPWL in view of Kim discloses: "The process of claim 33, wherein when a new terminal joins said group, it includes the step of selecting one of the other terminals in the group for exchanging said publicly accessible information with said new terminal joining the group." *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor communicates with new member publicly and updates the tree and computes the new group key and broadcasts it)*

14.   Claims 48 through 64 are rejected under 35 U.S.C. 103(a) as being unpatentable over Enhanced Protection over Wireless Lans (copyright February 2000, NoWiresNeeded) hereinafter called EPWL in view of Kim et al. Simple and fault-Tolerant Agreement for Dynamic Collaborative Groups (by Kim, Perrig and Tsudik copyright 2000 ACM) hereinafter called Kim.

As per claim 48, EPWL in view of Kim discloses: "A wireless network for secure communication among a group of terminals," *(EPWL, page 6, right hand column, lines 19 through 25, client and access points, i.e. terminals, communicate in a security enhanced 802.11 authentication protocol, hence communicate over a wireless network)* "wherein such terminals exchange information ciphered by means of at least one key," *(EPWL, page 6, right hand column, lines 10 through 12, each station i.e. terminal generates an encryption key using the Diffie-Hellman key agreement algorithm)* but fails to disclose expressly "comprising terminals in said group configured for generating said

at least one key independently at each terminal by means of a protocol of the group key

agreement type."

Kim discloses "comprising terminals in said group configured for generating said

at least one key independently at each terminal by means of a protocol of the group key

agreement type." *(Kim, page 235, right hand column, lines 30 through 34, group key*

management protocols are used)

EPWL and Kim are analogous art because they are from the same field of

endeavor of wireless communication.

It would have been obvious to one of ordinary skill in the art at the time of the

invention to incorporate the method for secure key exchange as described by EPWL

and the group key agreement method as taught by Kim because group key prevents

network from a single point of failure and therefore less attractive for attack *(Kim, page*

235, lines 14 through 18).

As per claim 49, EPWL in view of Kim discloses: "The network of claim 48,

wherein the terminals in said group are configured for: generating, at each said terminal

in said group, respective secret local data and maintaining said local data secret at said

terminal; *(EPWL, page 6, right hand column, lines 10 through 12, each station i.e.*

terminal generates an encryption key using the Diffie-Hellman key agreement algorithm,

this encryption key is secret data) exchanging publicly accessible information among

the terminals in said group; *(EPWL, page 6, right hand column, lines 7 through 8, each*

station i.e. terminal exchanges data without a need for secure a channel hence publicly

accessible information is exchanged among terminals in said group) and generating,

independently at each said terminal in the group, said at least one key on the basis of

said respective local data maintained secret at each said terminal and said publicly

accessible information." *(EPWL, page 6, right hand column, lines 7 through 16, each*

station i.e. terminal generates an encryption key using the Diffie-Hellman key

agreement algorithm from the information exchanged)

As per claim 50, EPWL in view of Kim discloses: "The network of claim 49,

wherein the terminals in said group are configured for incorporating to said publicly

accessible information coded information representative of each terminal in said group,

whereby generation of said at least one key is contributed by all the terminals in said

group." *(Kim, page 238, right hand column, lines 1 through 10, each member generates*

its own key which is a part of the group key, since each member knows the other keys

on the path each generates an intermediate key the root will create the root will create

the group key)

As per claim 51, EPWL in view of Kim discloses: "The network of claim 49,

wherein the terminals in said group are configured for: encoding each terminal in said

group by means of respective labels; and generating a vector of the labels of all the

terminals in said group, *(Kim, page 238, left hand column, lines 43 through 50, each*

member can compute and stores the identical tree which is the structure of the group, a

tree is a vector) wherein said vector is included in said publicly accessible information

exchanged among the terminals in said group." *(Kim, page 239, left hand column, lines*

1 through 5, sponsor broadcasts the tree)

As per claim 52, "The network of claim 49, wherein the terminals in said group

are configured for exchanging among them publicly accessible information

representative of a tree-structure for generating said at least one key." *(Kim, page 238,*

right hand column, lines 1 through 10, each member generates its own key which is a

part of the group key, each member knows all the keys from the path of its leaf)

As per claim 53, EPWL in view of Kim discloses: "The network of claim 48,

wherein the terminals in said group are configured for generating said at least one key

independently at each said terminal in said group by means of a Diffie-Hellman group

algorithm." *(EPWL, page 6, right hand column, lines 10 through 13, each station i.e.*

terminal generates an encryption key using the Diffie-Hellman key agreement algorithm)

As per claim 54, EPWL in view of Kim discloses: "The network of claim 53,

wherein said algorithm is the TGDH algorithm." *(Kim, page 238, left hand column, line*

21, TGDH algorithm protocols used)

As per claim 55, EPWL in view of Kim discloses: "The network of claim 48,

wherein the terminals in said group are configured for authenticating themselves by

means of digital authentication information." *(Kim, page 238, right hand column, lines 43*

through 48, a new member sends a join request to join group, page 238, left hand

column, lines 13 through 16, all communication is digitally signed hence digitally

authenticated)

As per claim 56, EPWL in view of Kim discloses: "The network of claim 55,

wherein the terminals in said group are configured for authenticating themselves by

means of a digital certificate." *(Kim, page 238, right hand column, lines 43 through 48, a*

new member sends a join request to join group, page 238, left hand column, lines 13

through 16, all communication is digitally signed hence digital certificate)

As per claim 57, EPWL in view of Kim discloses: "The network of claim 49,

wherein the terminals in said group are configured for exchanging said publicly

accessible information by means of information packets." *(Kim, page 235, right hand*

column, line 1, members are spread through the internet, internet communication is via

packets)

As per claim 58, EPWL in view of Kim discloses: "The network of claim 49,

wherein the terminals in said group are configured for fragmenting said publicly

accessible information over a plurality of information packets." *(Kim, page 235, right*

hand column, line 1, members are spread through the internet, internet communication

is via TCP/IP, packets in TCP are fragmented into the IP layer)

As per claim 59, EPWL in view of Kim discloses: "The network of claim 49, wherein the terminals in said group are configured for authenticating themselves by means of digital authentication information, *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digitally authenticated)* fragmenting said publicly accessible information over a plurality of information packets and associating said authentication information with all of said packets." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via TCP/IP, packets in TCP are fragmented into the IP layer)*

As per claim 60, EPWL in view of Kim discloses: "The network of claim 49, wherein the terminals in said group are configured for authenticating themselves by means of digital authentication information, *(Kim, page 238, right hand column, lines 43 through 48, a new member sends a join request to join group, page 238, left hand column, lines 13 through 16, all communication is digitally signed hence digitally authenticated)* fragmenting said publicly accessible information over a plurality of information packets and including said digital authentication information with one of said packets, whereby the remaining part of said plurality of packets comprises a lower protocol layer conveying information resulting from said fragmentation." *(Kim, page 235, right hand column, line 1, members are spread through the internet, internet communication is via TCP/IP, packets in TCP are fragmented into the IP layer, hence*

creating a plurality of packets at a lower protocol)

As per claim 61, EPWL in view of Kim discloses: "The network of claim 48, wherein the terminals in said group are configured for generating at least one message selected from the group consisting of: a join message generated when said terminal enters said group and conveying information that merged with other information provided by all the other terminals in said group is adapted to generate said at least one key; *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor updates the tree and computes the new group key and broadcasts it)* a key message generated during the generation of said at least one key and containing data that respective terminals other than a new terminal joining said group have to provide for generating said at least one key; *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor updates the tree and computes the new group key and broadcasts it, the sponsor can compute the new group key since it knows all the necessary blinded keys)* and a leave message generated to notify the other terminals in said group that the source terminal is leaving the group." *(Kim, page 239, section 5.3, when a member leaves new group key is computed by sponsor and broadcasted so other members can compute the knew group key and update the tree accordingly)*

As per claim 62, EPWL in view of Kim discloses: "The network of claim 48, wherein the terminals in said group are configured for selecting, when a new terminal joins said group, one of the other terminals in the group for exchanging said publicly accessible information with said new terminal joining the group." *(Kim, page 238, right hand column, lines 43 through page 239, left hand column, line 5, a new member sends a join request to join group, sponsor communicates with new member publicly and updates the tree and computes the new group key and broadcasts it)*

As per claim 63, EPWL in view of Kim discloses: "The network of claim 48, comprising a network according to the 802.11 standard." *(EPWL, page 6, right hand column, lines 19 through 25, client and access points communicate in a security enhanced 802.11 authentication protocol, hence following the 802.11 standard)*

As per claim 64, EPWL in view of Kim discloses: "A computer program product, directly loadable in the memory of at least one computer and including software code portions adapted for implementing the method of any one of claims 33-47." *(EPWL, page 6, right hand column, lines 7 through 25, each station with AirLock software, which is a computer program product loaded in memory, is able to communicate securely with each other, AirLock software uses the Diffie-Hellman key agreement algorithm to generate an encryption key which is the additional limitation in claim 37, claim 37 is dependent on claim 33 which is rejected above by EPWL in view of Kim)*

Conclusion

15.   The following prior art made of record and not relied upon is cited to establish the

level of skill in the applicant's art and those arts considered reasonably pertinent to

applicant's disclosure. See **MPEP 707.05(c)**.

The following reference teaches execution of trial data

US 6363154

US 6091820

US 5668877

Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Simon Kanaan whose telephone number is (571) 270-

3906. The examiner can normally be reached on Monday to Friday 8:30 AM to 5:00

PM.

If attempts to reach the above noted Examiner by telephone are unsuccessful,

the Examiner's supervisor, Thomas Pham, can be reached at the following telephone

number: (571) 272-3689.

The fax phone number for the organization where this application or proceeding

is assigned is 571-273-8300. Information regarding the status of an application may be

obtained from the Patent Application Information Retrieval (PAIR) system. Status

information for published applications may be obtained from either Private PAIR or

Public PAIR. Status information for unpublished applications is available through

Private PAIR only. For more information about the PAIR system, see http://pair-

direct.uspto.gov. Should you have questions on access to the Private PAIR system,

contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

August 20, 2008   Simon Kanaan
                                                                   Examiner
                                                                   Art Unit 4148

SPK

/THOMAS PHAM/
Supervisory Patent Examiner, Art Unit 4148